DOI:10.1145/2714559

Vinton G. Cerf

There Is Nothing New under the Sun

By chance, I was visiting the Folger Shakespeare Library^a last December where a unique manuscript was on display. It is called the Voynich Manuscript^b and all indications are it was written sometime

between 1410 and 1430. No one has succeeded in decoding it. Among the many who have tried was William Friedman, the chief cryptologist for the National Security Agency at the time of its founding. Friedman and his wife, Elizabeth, were great authorities on antiquities and together published books on this and many other topics. Of note is a book on Shakespearean Ciphers published in 1957^c exploring the use of ciphers in Shakespeare's works and contemporary writings.

I was interested to learn there are many books and manuscripts devoted to this mysterious codex. A brief Web search yielded a bibliography of many such works.^d Friedman ultimately concluded this was not a cipher but rather a language invented, *de novo*, whose structure and alphabet were unknown. In what I gather is typical of Friedman, he published his opinion on this manuscript as an anagram of the last paragraph in his article on acrostics and anagrams found in Chaucer's *Canterbury Tales*.^e Properly rearranged, the anagram reads:

"The Voynich MS was an early attempt to construct an artificial or universal language of the a priori type."

Friedman also drew one of our com-

puter science heroes into the fray, John Von Neumann. A photo of the two of them conferring on this topic was on display at the Folger. There is no indication that Von Neumann, a brilliant polymath in his own right, was any more able than Friedman to crack the code.

I was frankly astonished to learn that Francis Bacon devised a binary encoding scheme and wrote freely about it in a book published in 1623.^f In effect, Bacon proposed that one could hide secret messages in what appears to be ordinary text (or any other images) in which two distinct "characters" could be discerned, if you knew what to look for. He devised a five-bit binary method to encode the letters of the alphabet. For example, he would use two typefaces as the bits of the code, say, **W** and **W**. Bacon referred to each typeface as "A" and "B." He would encode the letter "a" as "AAAAA" and the letter "b" as "AAAAB," and "c" as AAABA, and so on through the alphabet. The actual image of the letter "a" could appear as **"theme"** since all five letters are in the bolder typeface (**AAAAA**). Of course, any five letters would do, and could be part of a word, all of a word, broken across two words. The letter "b" could be encoded as **"theme"** since this word is written as "AAAAB" in Bacon's "bilateral" code. Any pair of subtle differences could be used to hide the message—a form of steganography. Of course the encoding need not consist of five-letter words. "abc" could be encoded as: the hidden

message and would be read out as:

/the hi/ddenm/essag/e.../AAAA/AAAAB/AAABA/...

Examples at the Folger exhibit included a piece of sheet music in which the legs of the notes were either complete or slightly broken to represent the two "typefaces" of the binary code.

Showing my lack of knowledge of cryptography, I was quite surprised to realize that centuries before George Boole and Charles Babbage, the notion of binary encoding was well known and apparently even used!

Secret writing was devised in antiquity. Julius Caesar was known to use a simple rotational cipher (for example, "go back three letters" so that "def" would be written as "abc") so that this kind of writing is called Caesar Cipher. Of course, there are even older examples of secret writing. I need to re-read David Kahn's famous book^g on this subject.

Returning to binary for a moment, one is drawn to the possibility of using other systems than binary, not to encode, but to compute. As 2015 unfolds, I await further progress on quantum computing because there are increasing reports that the field is rapidly advancing. Between that and the neuromorphic chips that have been developed, one is expecting some very interesting research results for the rest of this year and, indeed, the decade. ■

g D. Kahn. *The Codebreakers—The Story of Secret Writing*. (1996), ISBN 0-684-83130-9.

Vinton G. Cerf is vice president and Chief Internet Evangelist at Google.

Copyright held by author.

a <http://www.folger.edu/>

b <http://brbl-dl.library.yale.edu/vufind/Record/3519597>

c W. and E. Friedman. *The Shakespearean Ciphers Examined*. Cambridge Univ. Press, 1957.

d <http://www.ic.unicamp.br/~stolfi/voynich/mirror/reeds/bib.html>

e Friedman, W.F., and Friedman, E.S. *Acrostics, Anagrams, and Chaucer*. (1959), 1–20.

f F. Bacon (1561–1626). *De Dignitate & augmentis scientiarum*, John Havilland, 1623.